Curated Web-of-Trust keyrings for free software projects: A case study on Debian's experience

Gunnar Wolf

LibrePlanet 2018; Cambridge, MA, USA; March 24-25 2018

Contenidos

The Debian keyrings: a *curated Web of Trust*

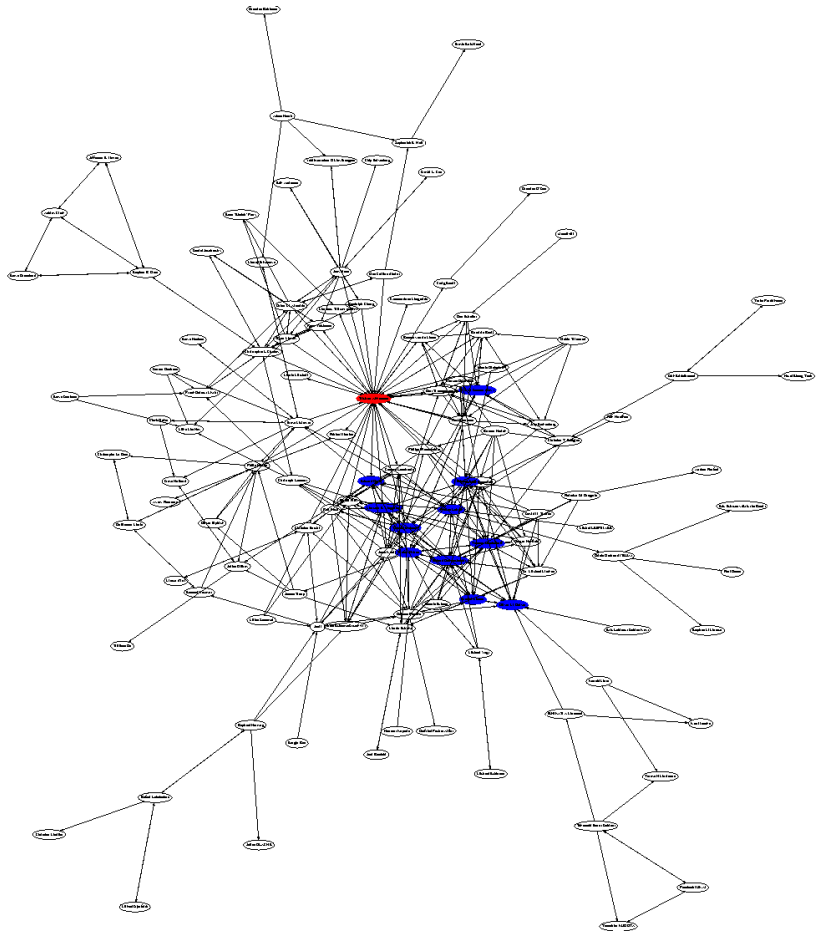
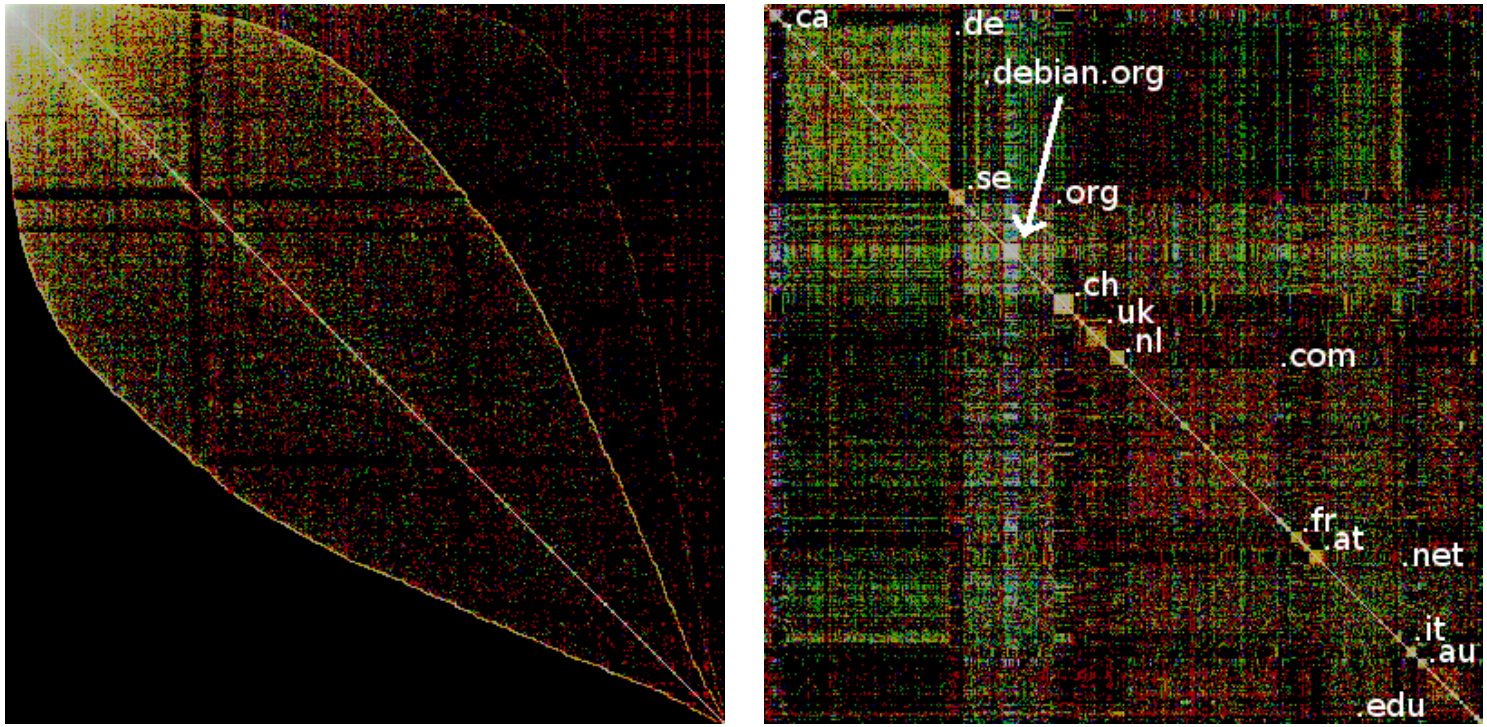


Figure: Graphical representation of the *strong set* of the Debian keyring back in 2000

Social studies from transitive trust graphs — And Debian's relative weight



(a) Whole "leaf"

(b) Sorted by TLD

Figure: Webs of Trust can teach us quite a bit - *Dissecting the Leaf of Trust* (Cederlöf 2008)

Work started after a big migration...

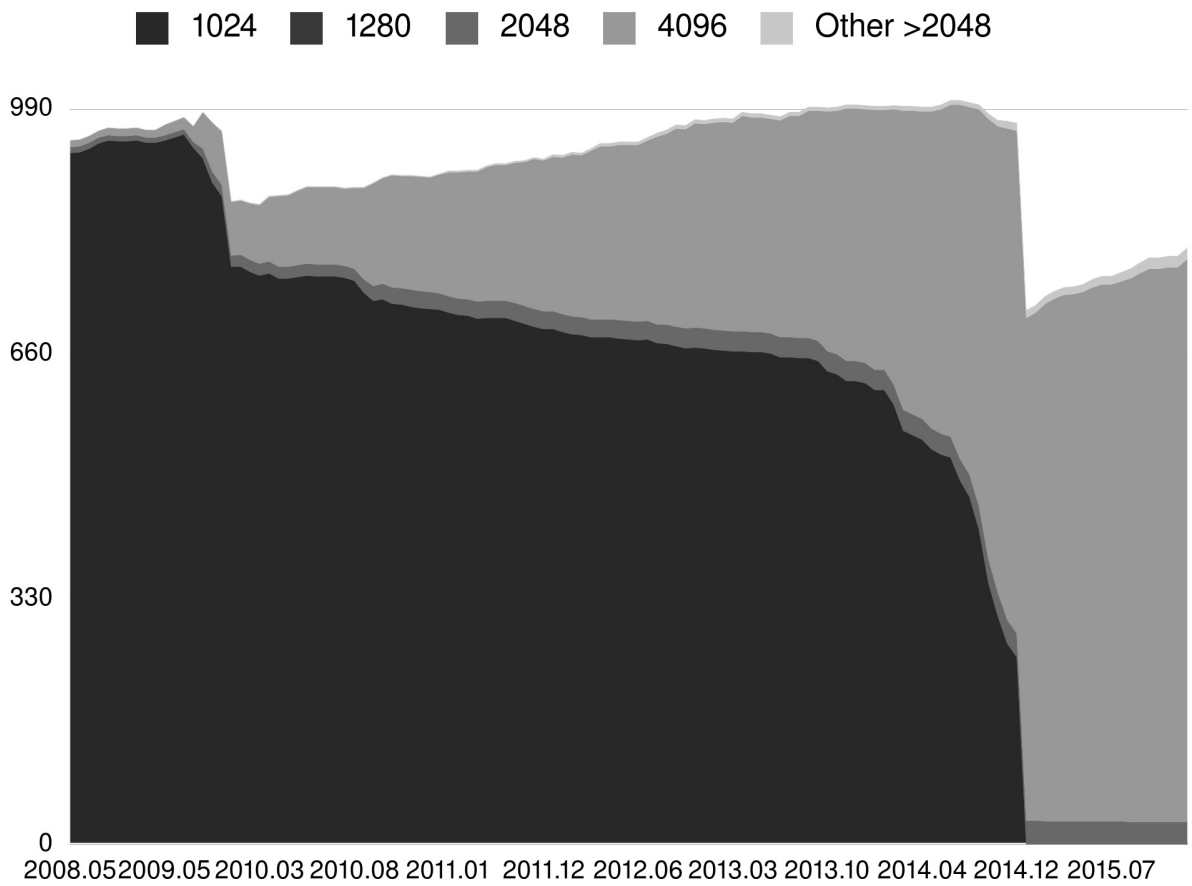


Figure: Breakdown of the Debian keyrings by key length, showing the migration away from short keys (<2048 bits)

Out of curiosity, the shape of the keyring

- Played with giving the keyring to `graphviz`
  - Might not be the best tool
  - Graph orientation and general shape is not *stable*
  - ...But the results are interesting nonetheless!
- Keys are nodes, signatures are edges
- Of course, it looks like a simple, useless blob...

Just a simple, boring blob: Debian Developers, 2015.01.01

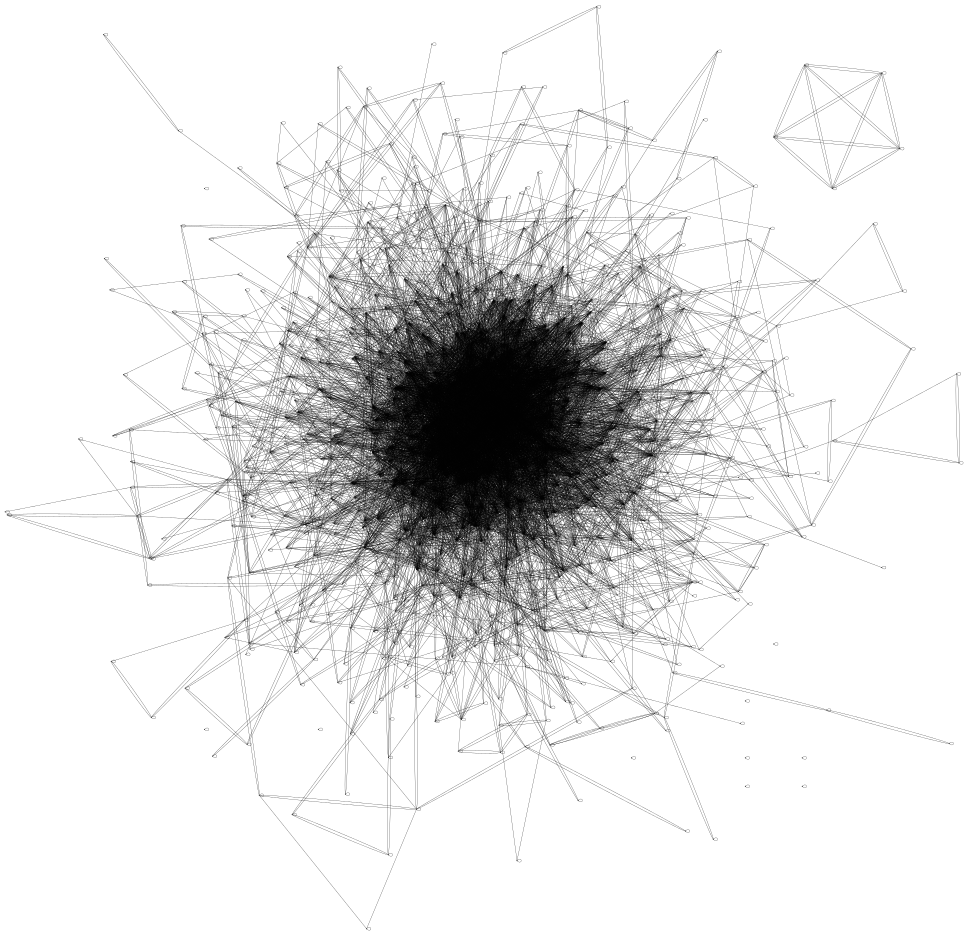


Figure: Our WoT — A maze of twisty passages, all alike

A *fun* blob: Debian Developers, January 2014

Thanks to having everything under Git (version control), we have a handy window to the past...

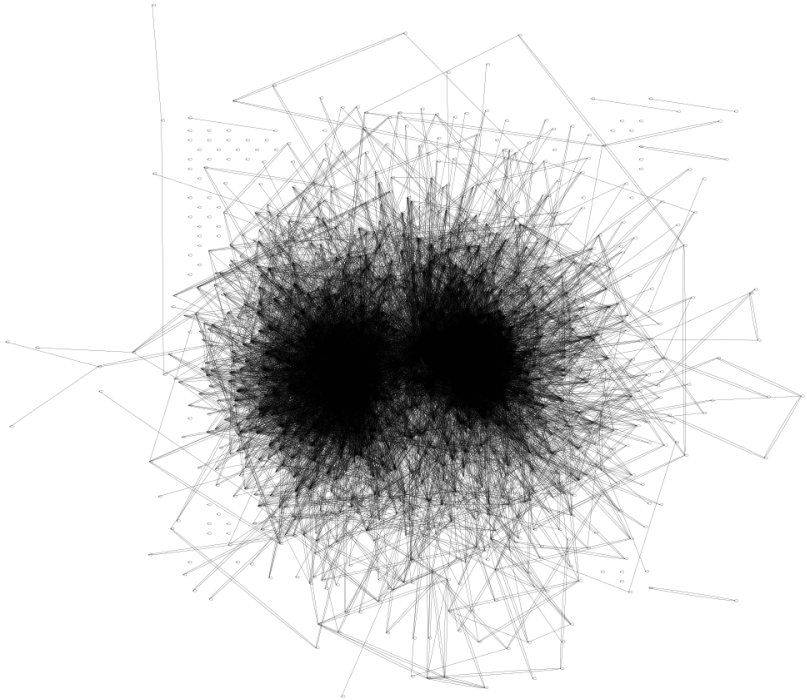
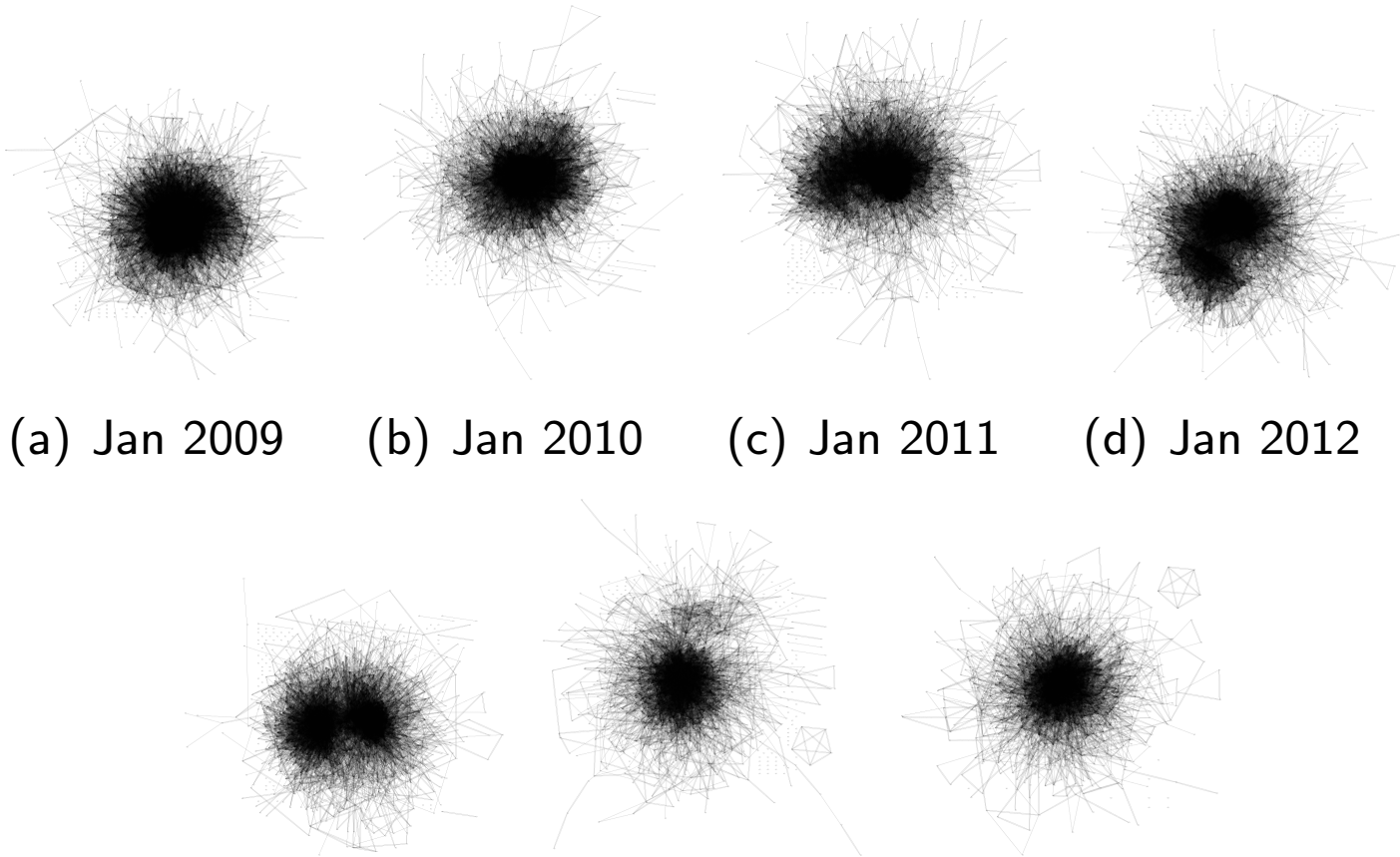


Figure: It's ALIVE!!!

- What does this split mean?
- Why did it appear?
- Where does it come from?
- How did it get there?
- When did it appear?

Evolution of the keyring



(a) Jan 2009 (b) Jan 2010 (c) Jan 2011 (d) Jan 2012

(e) Jan 2014 (f) Dec 2014 (g) Jan 2015

Figure: Snapshots of the Debian keyring evolution at different points in time

Contenidos

Hypothesis: Keyring aging?

- Leading to, and mostly during 2014, a huge portion of our keyring was replaced
  - One of the "blobs" marks older keys, the other new replacements?
  - But why the split began as early as 2011?
  - Note that nodes are grouped by their *cross-signatures* not by the key age (hence a 1024D key could be in the "younger" group and be expired!)
- Or it marks a *generation* of Debian Developers, slowly reducing their involvement?

Lets add some color!

- Nodes are irrelevant (`point`), only edges are important
- Edges represent key signatures; color denotes signature age WRT the point in time the snapshot was *taken*

Table: Color key for the resulting graphs

Blue	Less than one year
Green	1 to 2 years
Yellow	2 to 3 years
Orange	3 to 4 years
Red	over 4 years old

Same old keyrings: 2014.01.12

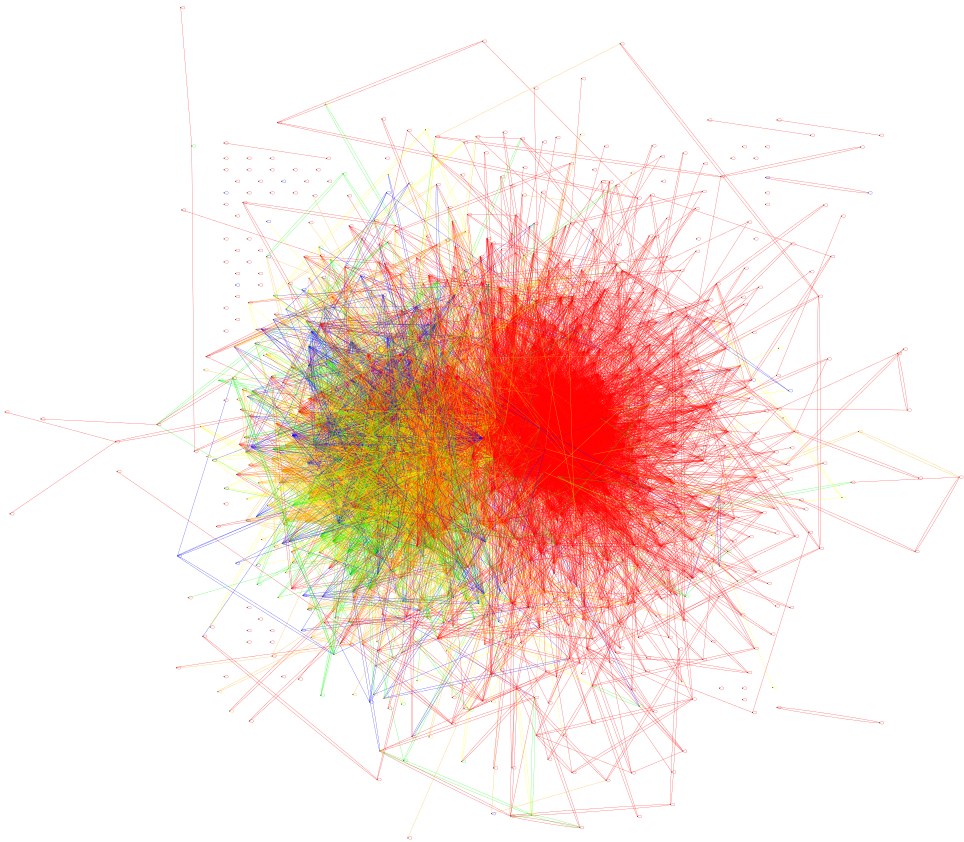


Figure: Big, red, disconnected blob

Same old keyrings: 2015.01.01

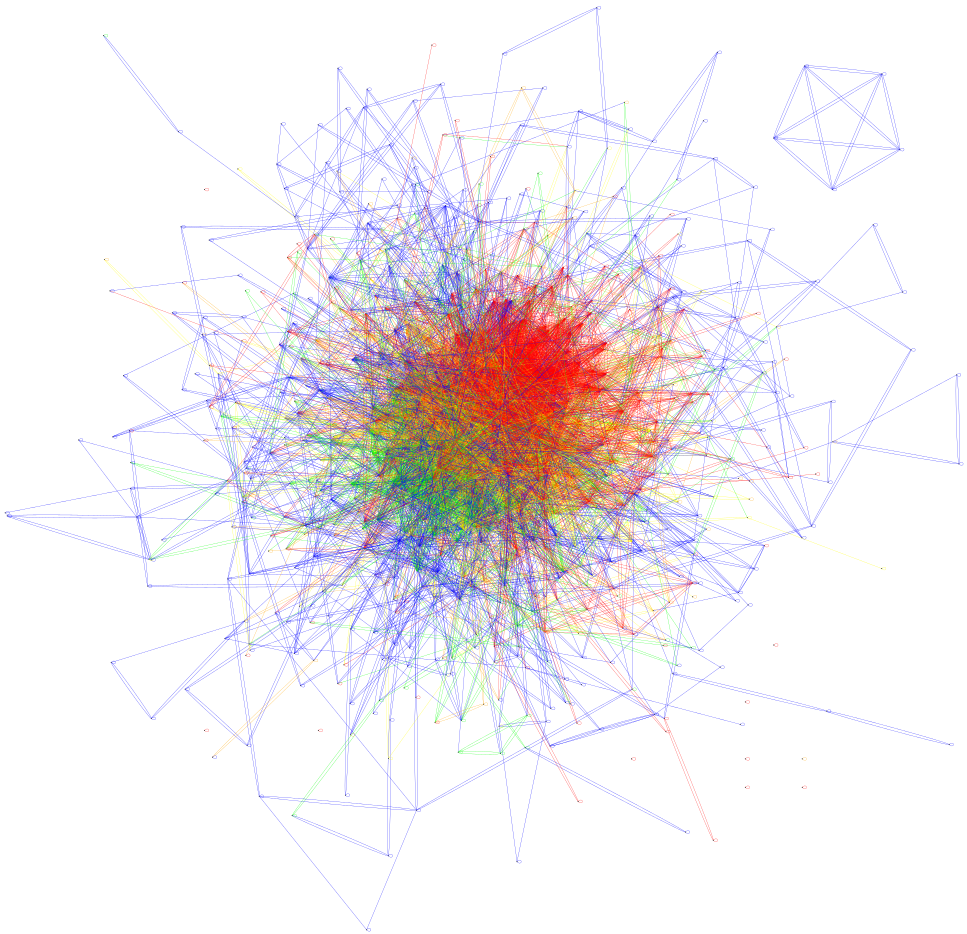
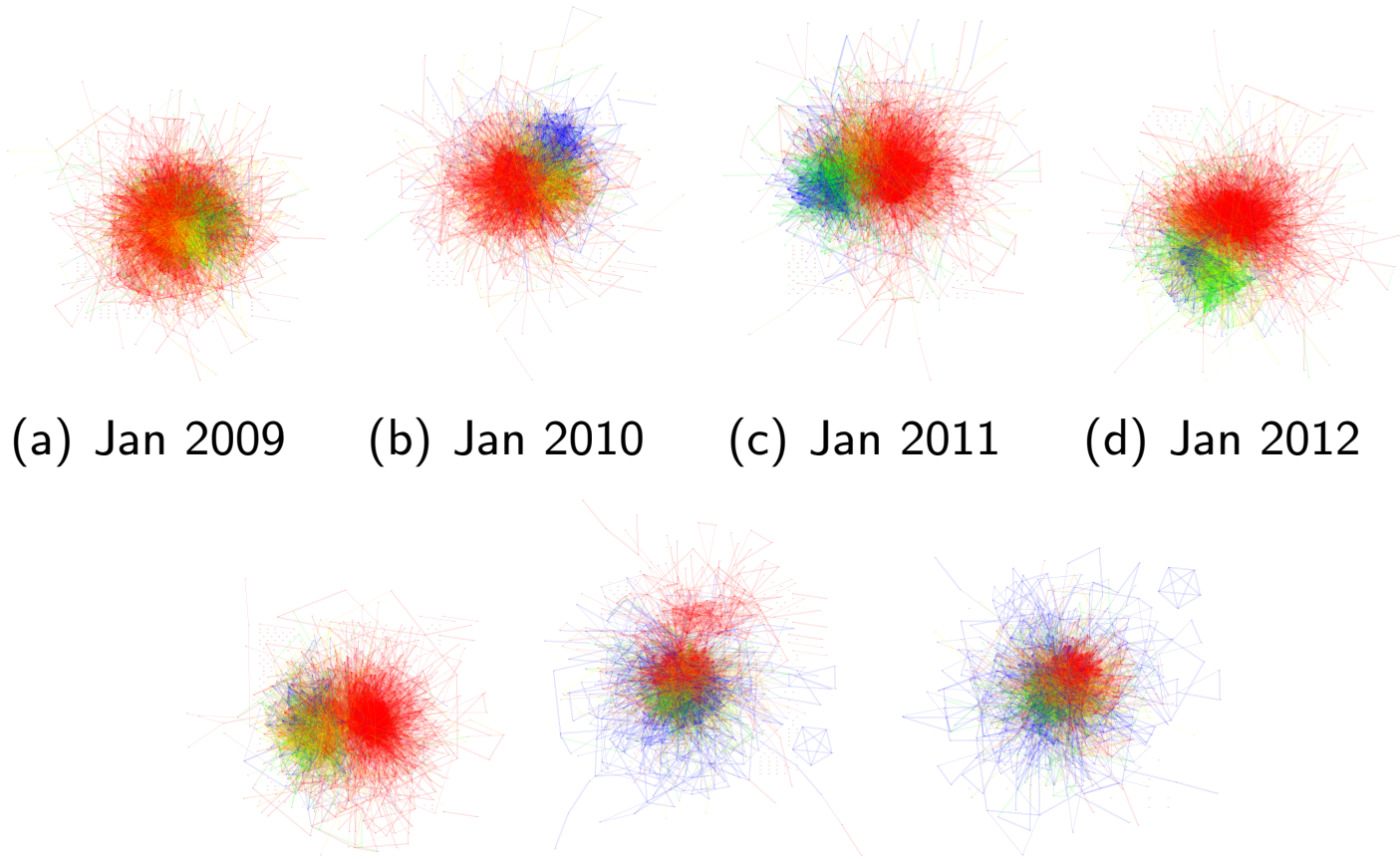


Figure: Still some areas dominated by color, but much better distributed

Same ten-keyring snapshot



(a) Jan 2009 (b) Jan 2010 (c) Jan 2011 (d) Jan 2012

(e) Jan 2014 (f) Dec 2014 (g) Jan 2015

Figure: Snapshots of the Debian keyring evolution at different points in time, showing signature age. Signature coloring is relative to each of the snapshots.

Contenidos

What is a KSP?

- At developer gatherings, such as DebConf
  - But also at other Free Software conferences — *Hint, hint!*
- Each participant of the KSP *verifies identity* of the others, *prepares for later* signing and mailing the key certification
  - Good practice! Use `caff` (in Debian's `signing-party` package)
- As a result, the overall strength of the WoT grows
  - Linking geographically-distant people, or people from different backgrounds...

Small-scale vs. Large-scale KSPs

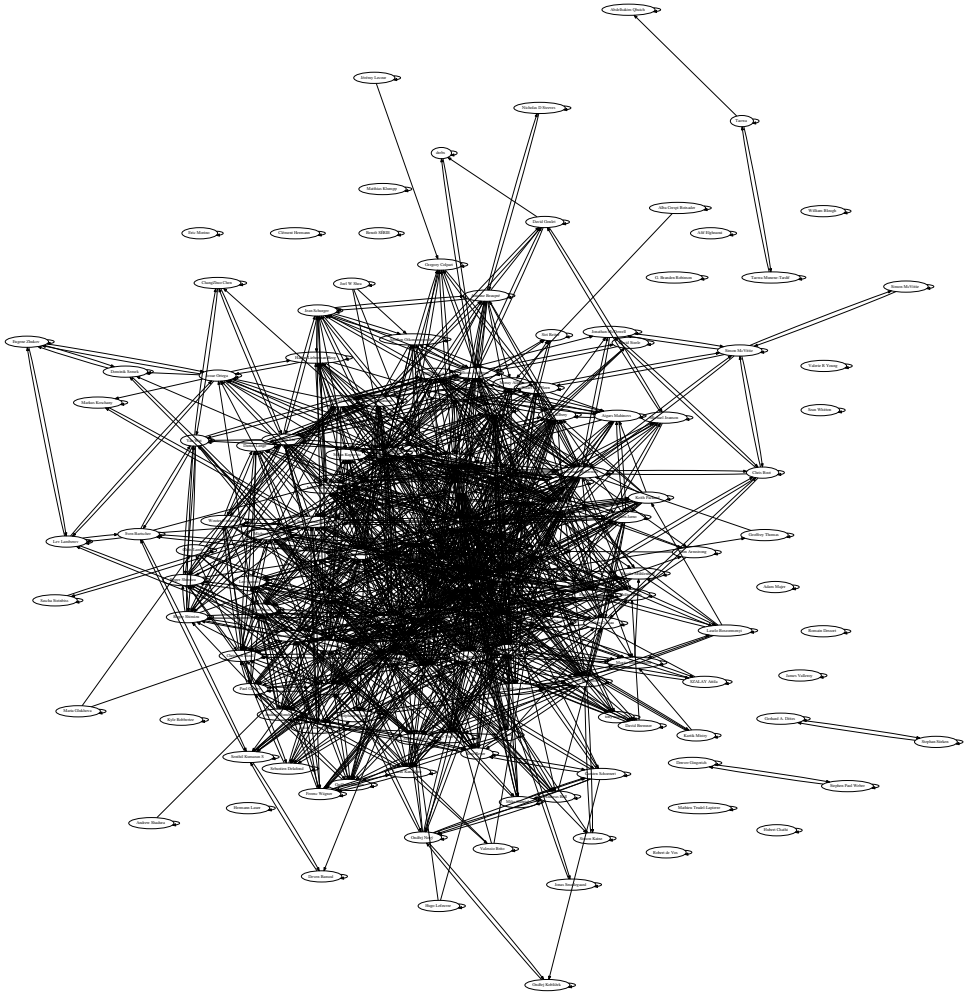
Sometimes, you expect to exchange only a few signatures... Things stay simple

1. Exchange paper slips with *full* fingerprints
2. Be *reasonably sure* of your peer's identity

Sometimes... It's too many people!

- KSP has to be arranged *in advance*!
- Verify integrity of a shared document with all fingerprints
- Just tick boxes (carefully!)

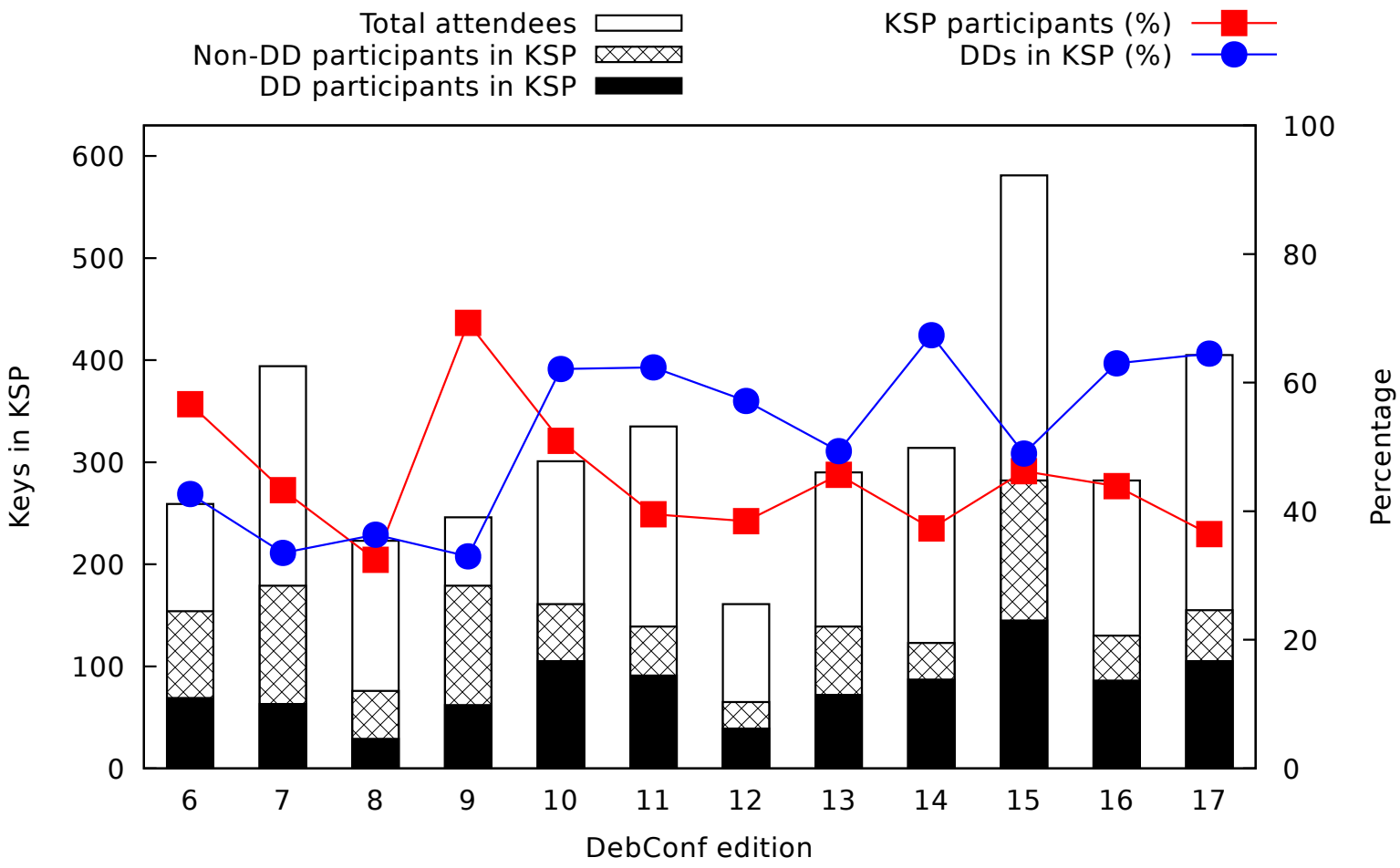
Studying each *big* KSP as a keyring



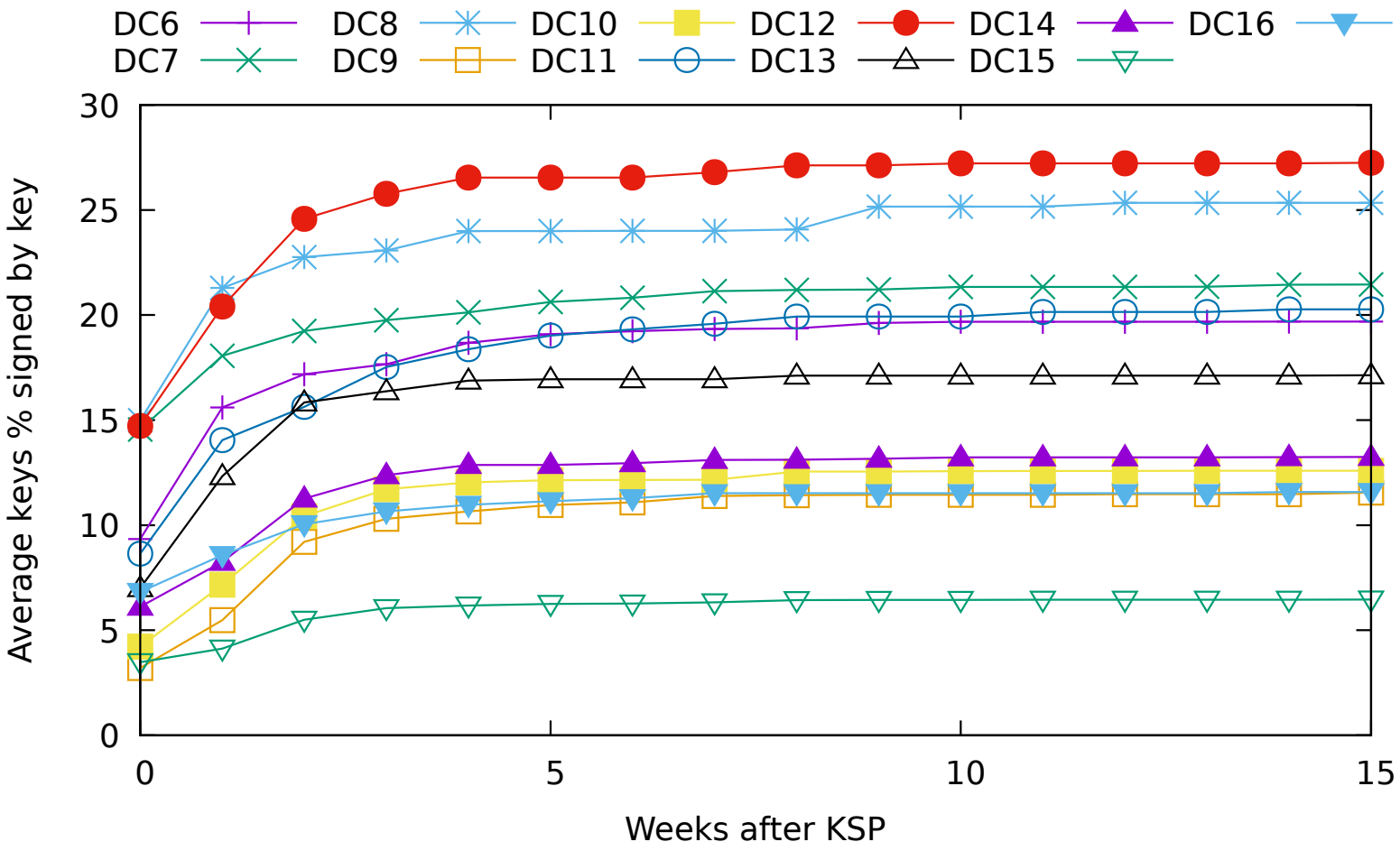
151 keys, 1638 signatures (including self)

Figure: Keyring for the DebConf17 KSP

DebConf KSPs by numbers — And some observed issues?



Increase of internal *signedness* after KSPs



Contenidos

What about *your project*?

- Applicability to other free software projects?
  - Correlate with events and trends spanning a wider population
  - Issue: Do we have a similar data source?
- Particularly for GNU/FSF: Work starting to start a CWoT
- Use from different data sources — After all, this is just social network graph analysis!
  - ...But needs to record interpersonal relations
  - Point in time for actions
  - Should preserve history (in our case, being in Git)
- In the future, it can document *issues* related to the history of your project...

Thanks!

Thanks for your attention!

Gunnar Wolf • gwolf@debian.org
AB41 C1C6 8AFD 668C A045 EBF8 673A 03E4 C1DB 921F

Debian Project
Instituto de Investigaciones Económicas (UNAM)